



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/755,037	01/08/2001	Terry Skemer	TR-053	4654
7590	01/03/2006		EXAMINER	
TROPIC NETWORKS INC. Attention: Dr. Victoria Donnelly 135 Michael Cowpland Drive Kanata, ON K2M 2E9 CANADA			SIMITOSKI, MICHAEL J	
			ART UNIT	PAPER NUMBER
			2134	
DATE MAILED: 01/03/2006				

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/755,037	SKEMER, TERRY	
	Examiner	Art Unit	
	Michael J. Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 01 July 2005.
 2a) This action is FINAL. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-12 and 14-25 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 1-12 and 14-25 is/are rejected.
 7) Claim(s) _____ is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on 08 January 2001 is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s)/Mail Date. _____
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)
3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____	6) <input type="checkbox"/> Other: _____

DETAILED ACTION

1. The response of 7/1/2005 was received and considered.
2. Claims 1-3, 5-12 & 14-25 are pending.

Response to Arguments

3. Applicant's arguments with respect to claims 1-12 & 14-25 have been considered but are moot in view of the new ground(s) of rejection. However, as any of the previously cited references pertain to the amended claims, arguments will be provided.

Regarding claims 1, 3, 10, 12, 14-16, 18-23 & 25, Fuh discloses that the client and intranet are both connected to the Internet (col. 7, lines 21-23), therefore, it is inherent that Fuh discloses that the data packet is received for accessing at least one of a plurality of ISP networks because the Internet is made up of backbone networks, mid-level networks and stub networks (plurality of ISP networks). See the cited reference to LinuxGuruz. Therefore, simply that the method and system as claimed in the present invention *can* communicate with a plurality of ISP networks is not sufficient to overcome the Fuh reference.

Regarding the remaining claims, the amendatory language suggests that the inventive device/method authenticates data units for a plurality if ISP networks. The Fuh reference appears to *disclose* only a single target server, where data destined for that server is authorized/authenticated by the access control node. However, the Howard reference is cited for teaching that performing access control and authentication/authorization mechanisms at a node, where the node is delegated access authority from a plurality of servers/ISP networks, it well known in the art providing the capability for a single entry point to perform

Art Unit: 2134

authentication/authorization for requests (col. 1, lines 16-22, col. 3, lines 25-35, col. 9, lines 24-39 & Fig. 1). Therefore, it would have been obvious to modify Fuh to control access to multiple target servers on multiple networks, rather than the single disclosed target server. This gains the advantage of the user authenticating to one server, but allowing authenticated data transmission to multiple networks (servers on the Internet).

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1, 3, 12, 15 & 25 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent 6,463,474 to Fuh et al. (**Fuh**).

Regarding claims 1, 15 & 25, Fuh discloses receiving, at an access control node/authentication proxy, which is operatively coupled to a plurality of user networks (Fig. 4), a data unit/packet from a user located on one of the plurality of user networks (Fig. 4 & Fig. 7A #702), determining whether the data unit/packet requires authentication (Fig. 7A, #703, 706), if the data unit/packet requires authentication, determining whether authentication data/source IP address is locally stored in a local authorization table/authentication cache (Fig. 4) on the access control node/authentication proxy (Fig. 7A, #708), if the authentication data/source IP address is locally stored in the local authorization table/authentication cache (Fig. 4) on the access control

Art Unit: 2134

node, authenticating the data unit (Fig. 7A, #710, 712), if the authentication data/source IP address is not locally stored in the local authorization table/authentication cache (Fig. 4) on the access control node, determining whether the data unit is eligible for transmission to said at least one of the plurality of ISP networks/target server (Fig. 4) and if the data unit/packet is eligible for transmission, transmitting the data unit/packet from the access control node/authentication proxy to said at least one of the plurality of ISP networks (Fig. 7B, #728). Fuh further discloses that the client and intranet are both connected to the Internet (col. 7, lines 21-23), therefore, it is inherent that Fuh discloses that the data packet is received for accessing at least one of a plurality of ISP networks because the Internet is made up of backbone networks, mid-level networks and stub networks (plurality of ISP networks). See the cited reference to LinuxGuruz.

Regarding claim 3, Fuh discloses receiving, at an access control node/authentication proxy, an authentication message (col. 12, lines 43-44) for said data unit from the at least one of the plurality of ISP networks to permit the user to access said ISP network/target server (Fig. 7B, #730, 736, 740).

Regarding claim 12, Fuh discloses determining the content of the authenticated data unit at the access control node (col. 11, lines 46-48).

6. Claims 1, 15 & 25 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent 6,584,505 to Howard et al. (**Howard**).

Regarding claims 1, 15 & 25, Howard discloses receiving, at an access control node/authentication server, which is operatively connected to a plurality of user networks/Internet (Fig. 1 & col. 3, lines 12-16), a data unit from a user located on one of the

plurality of user networks for accessing at least one of the plurality of ISP networks/affiliate servers connected to the access network (Fig. 1 & col. 6, lines 46-52), determining whether the data unit requires authentication for accessing said at least one of the plurality of ISP networks (col. 6, lines 53-59), if the data unit requires authentication, determining whether authentication data is locally stored in the local authorization table on the access control node/authentication database (col. 8, lines 57-65), if the authentication data is locally stored in the local authorization table on the access control node, authenticating the data unit (col. 8, lines 66-67), if the authentication data is not locally stored in the local authorization table on the access control node, determining whether the data unit is eligible for transmission to said at least one of the plurality of ISP networks (col. 7, lines 12-26) and if the data unit is eligible for transmission, transmitting said data unit from the access control node to said at least one of the plurality of ISP networks (col. 8, lines 27-31).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. Claims 2, 6-7, 11, 17 & 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Fuh**, as applied to claims 1 & 15 above, in view of **Howard**.

Regarding claim 2, Fuh lacks interrogating the user for access information to a plurality of ISP networks. However, Howard teaches a similar method of delegating

Art Unit: 2134

authentication/authorization services to an authentication server, wherein the authentication server controls user access to a plurality of ISP networks/affiliate servers (Fig. 1) and contains a local authentication table/cross-reference table containing login information for the user (col. 9, lines 24-39). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Fuh to interrogate the user for access information to a plurality of ISP networks. One of ordinary skill in the art would have been motivated to perform such a modification to allow a single authentication device to give access to a plurality of Internet sites, as taught by Howard (col. 1, lines 16-22, col. 3, lines 25-35, col. 9, lines 24-39 & Fig. 1).

Regarding claims 6, 11 & 20, Fuh discloses storing the authenticated data unit in a local authorization table/cache on the access control node (Fig. 7B, #732), but lacks the local authorization table comprising the authenticated data for the plurality of ISP networks. However, Howard teaches a similar method of delegating authentication/authorization services to an authentication server, wherein the authentication server controls user access to a plurality of ISP networks/affiliate servers (Fig. 1) and contains a local authentication table/cross-reference table containing login information for the user (col. 9, lines 24-39). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Fuh to store authenticated data/access information for a plurality of ISP networks in the local authorization table. One of ordinary skill in the art would have been motivated to perform such a modification to allow a single authentication device to give access to a plurality of Internet sites, as taught by Howard (col. 1, lines 16-22, col. 3, lines 25-35, col. 9, lines 24-39 & Fig. 1).

Regarding claim 7, Fuh discloses searching the authenticated data units stored in the local authorization table/cache on the access control node (Fig. 7A, #708).

Regarding claim 17, Fuh discloses searching the authenticated data unit locally stored on the access control node (Fig. 7A, #708), but lacks a local authorization table for authorizing data units for said plurality of ISP networks. However, Howard teaches a similar method of delegating authentication/authorization services to an authentication server, wherein the authentication server controls user access to a plurality of ISP networks/affiliate servers (Fig. 1) and contains a local authentication table/cross-reference table containing login information for the user (col. 9, lines 24-39). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Fuh to store access information for a plurality of ISP networks. One of ordinary skill in the art would have been motivated to perform such a modification to allow a single authentication device to give access to a plurality of Internet sites, as taught by Howard (col. 1, lines 16-22, col. 3, lines 25-35, col. 9, lines 24-39 & Fig. 1).

9. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Fuh & Howard**, as applied to claim 2 above, in further view of U.S. Patent 5,491,752 to Kaufman et al. (**Kaufman**). Fuh, as modified above, lacks specifically encrypting the access information prior to transmitting it. However, Kaufman teaches that to avoid password eavesdropping, it is known to encrypt the password/access information (col. 3, lines 26-40). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to encrypt the

Art Unit: 2134

access information. One of ordinary skill in the art would have been motivated to perform such a modification to render eavesdropping useless, as taught by Kaufman (col. 3, lines 26-40).

10. Claims 8, 9 & 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Fuh** in view of **Howard** & “AAA PROTOCOLS: Authentication, Authorization and Accounting for the Internet”, by **Metz**. Fuh lacks explicitly communicating with the plurality of ISP networks and is silent regarding the particular AAA protocol used in the authentication server. However, Howard teaches a similar method of delegating authentication/authorization services to an authentication server, wherein the authentication server controls user access to a plurality of ISP networks/affiliate servers (Fig. 1) and contains a local authentication table/cross-reference table containing login information for the user (col. 9, lines 24-39). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Fuh to communicate with a plurality of ISP networks. One of ordinary skill in the art would have been motivated to perform such a modification to allow a single authentication device to give access to a plurality of Internet sites, as taught by Howard (col. 1, lines 16-22, col. 3, lines 25-35, col. 9, lines 24-39 & Fig. 1). Further, Metz teaches that RADIUS is the best-known and most widely used AAA protocol (p. 76, §RADIUS). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the remote authentication dial-in user service protocol in Fuh’s authorization server/AAA server and access control node (Fuh, col. 10, lines 49-58). One of ordinary skill in the art would have been motivated to perform such a modification to use a widely used AAA protocol, as taught by Metz (p. 76, §RADIUS).

11. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Fuh**, as applied to claim 3 above, in further view of U.S. Patent 5,546,387 to Larsson et al. (**Larsson**). Fuh, as modified above, lacks packet-labeling the data unit. However, Larsson teaches that data labeling is required in a packet network so that data packets can be uniquely assigned a connection and routed between nodes (col. 1, lines 16-27). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to packet-label the data unit. One of ordinary skill in the art would have been motivated to perform such a modification to uniquely assign the data unit a connection and route the data unit between nodes in a network, as taught by Larsson (col. 1, lines 16-27).

12. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Fuh**, as applied to claim 1 above, in further view of U.S. Patent 6,377,955 to Hartmann et al. (**Hartmann**). Fuh, as modified above, lacks collecting statistical usage information at the access node. However, Hartmann teaches that when network access servers/access nodes are part of an ISP, accurate accounting of connection time is required so customers are billed correctly (col. 1, lines 34-56). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to collect statistical usage information at the access node. One of ordinary skill in the art would have been motivated to perform such a modification to ensure accurate accounting of connection time so customers are billed correctly, as taught by Hartmann (col. 1, lines 34-56).

Art Unit: 2134

13. Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Fuh**, as applied to claim 15 above, in further view of U.S. Patent 5,903,564 to Ganmukhi et al. (**Ganmukhi**). Fuh lacks the user network interface including a plurality of ingress cards and the external network interface including an egress card. However, Ganmukhi teaches that ATM switches (devices for receiving and sending packets) typically include ingress cards and egress cards to support multiple connections in transmitting data (col. 1, lines 13-29). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a plurality of ingress cards and an egress card. One of ordinary skill in the art would have been motivated to perform such a modification to support the transmission of packets from multiple connections, as taught by Ganmukhi (col. 1, lines 13-29).

14. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Fuh**, as applied to claim 15 above, in further view of U.S. Patent 6,311,275 to Jin et al. (**Jin**). Fuh lacks the authentication agent including network address assignment and release means. However, Jin teaches that in order for a network to communicate with the user, and IP address must be assigned, which can be done by the AAA server (col. 2, lines 34-44). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include, in the authentication agent/AAA server, means to assign and release IP addresses. One of ordinary skill in the art would have been motivated to perform such a modification to allow the network to communicate with the user, as taught by Jin (col. 2, lines 34-44).

15. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Fuh**, as applied to claim 15 above, in further view of U.S. Patent 6,466,977 to Sitaraman et al. (**Sitaraman**), **Hartmann** and U.S. Patent 6,510,454 to **Walukiewicz**. Fuh lacks service level enforcing means, network resource management means, statistical usage information and alarm-monitoring means. However, Sitaraman teaches that it is desirable to load balance among instances of AAA services and to route a user to a sub-service provider based on service level agreements (SLA) (col. 3, lines 14-41). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to further include service level enforcing means. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to load balance among instances of AAA services and to route users to sub-service providers based on SLAs, as taught by Sitaraman (col. 3, lines 14-41). Further, Sitaraman teaches that it is desirable to decide the AAA service/resource to use based on parameters such as quality of service, available bandwidth, etc. (col. 3, lines 14-41). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include network resource management means. One of ordinary skill in the art would have been motivated to perform such a modification because it is desirable to do so, as taught by Sitaraman (col. 3, lines 14-41). Further, Hartmann teaches that when network access servers/access nodes are part of an ISP, accurate accounting of connection time is required so customers are billed correctly (col. 1, lines 34-56). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include means for statistical usage collection. One of ordinary skill in the art would have been motivated to perform such a modification to ensure accurate accounting of connection time so customers are billed correctly,

Art Unit: 2134

as taught by Hartmann (col. 1, lines 34-56). Further, Walukiewicz teaches that network alarm monitoring is needed to quickly correct the problem via a technician or an automated algorithm (col. 1, lines 19-33). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include alarm-monitoring means. One of ordinary skill in the art would have been motivated to perform such a modification to correct problems via a technician or an automated algorithm, as taught by Walukiewicz (col. 1, lines 19-33).

16. Claims 21-22, as best understood, are rejected under 35 U.S.C. 103(a) as being unpatentable over **Fuh**, as applied to claim 15 above, in further view of “PPP Authentication Protocols” by Lloyd et al. (**Lloyd**). Fuh lacks the authentication agent employing a PAP or CHAP protocol. However, Lloyd teaches that PAP and CHAP are both well-known methods of verifying the identity of a peer (pages 1-8, §2-3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ a password authentication protocol or the challenge handshake authentication protocol client in the authentication agent. One of ordinary skill in the art would have been motivated to perform such a modification to verify the identity of a peer, as taught by Lloyd (pages 1-8, §2-3).

17. Claim 23, as best understood, is rejected under 35 U.S.C. 103(a) as being unpatentable over **Fuh**, as applied to claim 15 above, in further view of “An Access Control Protocol, Sometimes Called TACACS” by **Finseth**. Fuh, as modified above, lacks the authentication agent employing a terminal access controller access control system. However, Finseth teaches that TACACS is a protocol that allows an authentication server to receive a username and

Art Unit: 2134

password to accept or deny requests for access (page 1, ¶2-3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ a TACACS system in the authentication agent. One of ordinary skill in the art would have been motivated to perform such a modification to accept or deny requests for access on dial up lines, as taught by Finseth (page 1, ¶2-3).

Conclusion

18. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached at (571) 272-3838.

Any response to this action should be mailed to:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Or faxed to:

(571) 273-8300
(for formal communications intended for entry)

Or:

(571) 273-3841 (Examiner's fax, for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJS

MJS
December 16, 2005

David Y. Jung
Primary Examiner

DM
12/23/08